Freak Angriff auch unter Windows möglich

Sämtliche Windows-Versionen lassen sich über die jüngst bekanntgewordene Freak-Attacke angreifen. Das bestätigte Microsoft in einer Warnung. Unklar ist, wann die Lücke geschlossen wird.

Die Freak-Schwachstelle betrifft auch alle Versionen des Internet Explorers in sämtlichen Windows-Betriebssystemen. Das bestätigte Microsoft in einem entsprechenden Advisory. Der Windows-Hersteller macht zwar keine Angaben dazu, wann er Patches für die Sicherheitslücke veröffentlichen wolle, gibt aber Hinweise, wie die Freak-Lücke vorübergehend geschlossen werden könne. Dann können im Internet Explorer manche Webseiten jedoch nicht geöffnet werden. Außerdem gibt es Diskussionen darüber, wie gravierend die Lücke wirklich sei.

Mittlerweile hat Google das Update 41 für den Chrome-Browser unter Mac OS X veröffentlicht, die die Lücke schließt. Apple hat angekündigt, selbst an Patches für iOS und Mac OS X zu arbeiten, die nächste Woche veröffentlicht werden sollen. Für Googles Chrome unter Android gibt es noch kein Update und auch keine offiziellen Angaben dazu, wann ein entsprechender Patch zur Verfügung gestellt werden solle. Bislang gilt nur Mozillas Firefox-Browser als sicher. Auf der Webseite Freakattack.com können Nutzer prüfen, ob ihr Browser angreifbar ist.

Millionen Webseiten verwundbar

Mit Freak (Factoring attack on RSA-Export Keys) können Angreifer über präparierte Datenpakete eine Verbindung über eine schwache 512-Bit-Verschlüsselung zwischen Client und Server erzwingen. Solche Schlüssel lassen sich in etwa sieben Stunden knacken. Damit können Dritte auch den verschlüsselten Datenverkehr über HTTPS abhören.

Damit der Angriff funktioniert, muss der Server den entsprechenden uralten RSA-Export-Modus unterstützen. Erschreckenderweise tun das nach wie vor erstaunlich viele Server. Laut Scans der Universität von Michigan sind etwa 37 Prozent der 14 Millionen TLS-Server für diesen Angriff verwundbar. Viele bekannte Webseiten haben den Fehler aber nicht, etwa Google oder Facebook.

Viele Bibliotheken betroffen

Wie sich bei den Untersuchungen der Inria-Forscher herausstellte, akzeptieren sowohl OpenSSL als auch die TLS-Bibliothek von Apple und der Internet Explorer einen schwachen, temporären 512-Bit-RSA-Schlüssel im Export-Modus. Das funktioniert aufgrund eines Fehlers auch dann, wenn der Client keinen derartigen Schlüssel angefordert hat. Selbst das wäre nur ein kleines Problem, denn ein Angreifer müsste in diesem Modus den temporären RSA-Schlüssel innerhalb von Sekunden brechen, um die Verbindung praktisch anzugreifen. Obwohl das Knacken von 512-Bit-Schlüsseln nicht besonders schwer ist, dürfte das nur für wenige Angreifer praktikabel sein. Deshalb gilt Freak unter einigen Experten als nicht allzu gravierend.

Doch es kommt ein weiteres Problem hinzu: Gängige Webserver wie beispielsweise Apache generieren den temporären 512-Bit-Schlüssel nicht live, sondern cachen ihn für die gesamte Laufzeit eines Serverprozesses. Da die Freak-Lücke mehrere Jahre lang existierte, könnten

Angreifer die Lücke bereits seit Jahren ausgenutzt haben. In OpenSSL wurde der Bug mit den RSA-Export-Ciphern als CVE-2015-0204 mit den Updates erst im Januar 2015 behoben. Die aktuelle Version 1.0.2 sowie die jüngsten Fixes der älteren Versionszweige (1.0.1l, 1.0.0q, 0.9.8ze) sind nicht mehr betroffen.

Relikt aus dem Crypto-Krieg

Die Export-Verschlüsselungsalgorithmen in TLS sind ein Relikt aus den 90er Jahren. Die USA hatten damals Gesetze, die die Nutzung starker Kryptographie und insbesondere deren Export einschränkten. Die politischen Auseinandersetzungen um derartige Einschränkungen von Verschlüsselungstechnik bezeichnete man auch als Crypto Wars. Mit dem TLS-Vorgänger SSL wurden Algorithmen eingeführt, die absichtlich schwache Schlüssel nutzten. Eigentlich sollten die Export-Cipher heute nirgends mehr zum Einsatz kommen, doch sie werden offenbar nach wie vor von aktueller Software unterstützt.